The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

10/31/2013

SUBJECT: Multiple Vulnerabilities in Mozilla Products Could Allow Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Mozilla Firefox, Thunderbird, and SeaMonkey applications, which could allow remote code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Thunderbird is an email client. Mozilla SeaMonkey is a cross platform Internet suite of tools ranging from a web browser to an email client. Successful exploitation of these vulnerabilities could result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Firefox versions prior to 25.0
- Firefox Extended Support Release (ESR) versions prior to 17.0.10
- Thunderbird versions prior to 24.1
- Thunderbird Extended Support Release (ESR) versions prior to 17.0.10
- SeaMonkey versions prior to 2.22

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:

Multiple vulnerabilities have been discovered in Mozilla Firefox, Thunderbird, and SeaMonkey. The details of these vulnerabilities are as follows:

- A use-after-free vulnerability occurs due to an error in the HTML document templates. Specifically, this issue affects the 'nsContentUtils::ContentIsHostIncludingDescendantOf()' function. This leads to a potentially exploitable crash. [CVE-2013-5603] [MFSA 2013-102]
- A memory-corruption vulnerability occurs within the JavaScript engine when using workers with direct proxies. Specifically, this issue affects the 'Worker::SetEventListener()' function. This leads to a potentially exploitable crash. [CVE-2013-5602] [MFSA 2013-101]
- Multiple use-after-free vulnerabilities occur due to missing strong references in the browsing engine. Specifically, these issues affect the 'nsIPresShell::GetPresContext()', 'nsIOService::NewChannelFromURIWithProxyFlags()' and 'nsEventListenerManager::SetEventHandler()' functions. This leads to a potentially exploitable crash. [CVE-2013-5599, CVE-2013-5600, CVE-2013-5601] [MFSA 2013-100]
- A security-bypass vulnerability exists because it fails to perform validation checks on 'PDF.js' javascript and appends an iframe into an embedded PDF. An attacker can exploit this issue to load local or chrome privileged files and objects within the embedded PDF object. This can lead to information disclosure of local system files. [CVE-2013-5598] [MFSA 2013-99]
- A use-after-free vulnerability occurs due to an error in the state change events when updating the offline cache. Specifically, this issue affects the 'nsDocLoader::doStopDocumentLoad()' function. This leads to a potentially exploitable crash. [CVE-2013-5597] [MFSA 2013-98]
- A denial-of-service vulnerability occurs due to a race-condition error when a cycle collected image object is released on the wrong thread during decoding. An attacker can exploit this issue to crash extremely large pages, causing a denial-of-service condition. This leads to a potentially exploitable crash. [CVE-2013-5596] [MFSA 2013-97]
- A buffer-overflow vulnerability affects the javaScript engine. Specifically, this issue occurs due to incorrect allocation of memory for certain functions.[CVE-2013-5595] [MFSA 2013-96]
- A denial-of-service vulnerability occurs due to an access-violation error with an uninitialized data during the Extensible Stylesheet Language Transformation (XSLT) processing. Specifically, this issue affects the 'txXPathNodeUtils::getBaseURI()' function. This leads to a potentially exploitable crash.
- [CVE-2013-5604] [MFSA 2013-95]
- An URI-spoofing vulnerability occurs because it fails to validate user-supplied input submitted to the SELECT element. This may allow attackers to conduct spoofing attacks by using a specially crafted URI. [CVE-2013-5593] [MFSA 2013-94]
- Several memory safety bugs in the browser engine, some of which showed evidence of memory-corruption vulnerabilities.
  [CVE-2013-5592, CVE-2013-5591, CVE-2013-5590] [MFSA 2013-93]

Successful exploitation of these vulnerabilities could result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data, or create new accounts with full user rights.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Upgrade vulnerable Mozilla products immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Do not open email attachments or click on URLs from unknown or untrusted sources.

- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Mozilla:

http://www.mozilla.org/security/announce/2013/mfsa2013-93.html

http://www.mozilla.org/security/announce/2013/mfsa2013-94.html

http://www.mozilla.org/security/announce/2013/mfsa2013-95.html

http://www.mozilla.org/security/announce/2013/mfsa2013-96.html

http://www.mozilla.org/security/announce/2013/mfsa2013-97.html

http://www.mozilla.org/security/announce/2013/mfsa2013-98.html

http://www.mozilla.org/security/announce/2013/mfsa2013-99.html

http://www.mozilla.org/security/announce/2013/mfsa2013-100.html

http://www.mozilla.org/security/announce/2013/mfsa2013-101.html

http://www.mozilla.org/security/announce/2013/mfsa2013-102.html

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5590

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5591

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5592

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5593

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5595

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5596

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5597

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5598

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5599

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5600

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5601

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5602

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5603

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5604

SecurityFocus:

http://www.securityfocus.com/bid/63405